

COPY



KEVIN JESPERSEN
ACTING ATTORNEY GENERAL OF NEW JERSEY
Division of Law
124 Halsey Street - 5th Floor
P.O. Box 45029

Newark, New Jersey 07101

Attorney for the Plaintiffs

By: Elliott M. Siebers – ID# 033582012

Russell M. Smith, Jr. – ID# 014202012

Deputy Attorneys General

Brian McDonough – ID# 026121980

John M. Falzone – ID# 017192003

Assistant Attorneys General

RECEIVED

FEB 14 2017

SUPERIOR COURT OF NJ
MERCER VICINAGE
CIVIL DIVISION

FILED

FEB 14 2017

SUPERIOR COURT OF NEW JERSEY
CHANCERY DIVISION, MERCER COUNTY
DOCKET NO. C-12-17

KEVIN JESPERSEN, Acting Attorney General of the
State of New Jersey, and STEVE C. LEE, Director of
the New Jersey Division of Consumer Affairs,

Plaintiffs,

v.

HORIZON HEALTHCARE SERVICES, INC., d/b/a
HORIZON BLUE CROSS BLUE SHIELD OF NEW
JERSEY,

Defendant.

Civil Action

COMPLAINT

Plaintiffs, Kevin Jespersen, Acting Attorney General of the State of New Jersey (“Attorney General”), with offices located at the Richard J. Hughes Justice Complex, 25 Market Street, Trenton, New Jersey, and Steve C. Lee, Director of the New Jersey Division of Consumer Affairs (“Director”), with offices located at 124 Halsey Street, Seventh Floor, Newark, New Jersey (collectively, “Plaintiffs”), by way of Complaint state:

PRELIMINARY STATEMENT

1. Horizon Healthcare Services, Inc. d/b/a Horizon Blue Cross Blue Shield of New Jersey (“Horizon BCBSNJ”) is and, at all relevant times, has been the largest health insurance company in the State of New Jersey (“New Jersey” or “State”), providing health insurance coverage to more than 3.7 million New Jersey residents.

2. As set forth in detail below, Horizon BCBSNJ has failed to protect certain members’ sensitive information, including electronic protected health information (“ePHI”), from data breaches.

3. As a result, Horizon BCBSNJ has violated the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 et seq. (“CFA”), and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, as well as the Department of Health and Human Services Regulations, 45 C.F.R. §160 et seq. (collectively, “HIPAA”).

4. The Attorney General and the Director commence this action to halt Horizon BCBSNJ’s unconscionable business practices; enforce compliance with HIPAA’s data security, privacy and administrative rules; and secure other authorized relief.

PARTIES AND JURISDICTION

5. The Attorney General is charged with the responsibility of enforcing the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 et seq. (“CFA”). The Director is charged with the responsibility of administering the CFA on behalf of the Attorney General.

6. The Attorney General as parens patriae for New Jersey and on behalf of the State in its sovereign capacity, may, pursuant to 42 U.S.C. § 1320d-5(d), enforce the provisions of HIPAA.

Plaintiffs provided prior written notice of this action to the Secretary of the United States Department of Health & Human Services, pursuant to 42 U.S.C. § 1320d-5(d)(4).

7. Pursuant to R. 4:3-2, venue is proper in Mercer County because Horizon BCBSNJ has maintained a business address and/or otherwise conducted business in this county.

8. Horizon BCBSNJ is a domestic corporation with headquarters located at 3 Penn Plaza East, Newark, New Jersey 07105 (“Newark Office”).

GENERAL ALLEGATIONS COMMON TO ALL COUNTS

9. Horizon BCBSNJ offers a variety of health insurance plans, including traditional indemnity and managed care plans, such as Health Maintenance Organization, Preferred Provider Organization and Point of Service plans, as well as Medicaid and Medicare coverage.

10. Through such plans, Horizon BCBSNJ provides health insurance coverage to more than 3.7 million New Jersey residents.

11. In servicing these plans, Horizon BCBSNJ maintains in electronic media, among other things, New Jersey residents’ names, addresses, dates of birth, identification numbers, Social Security Numbers, and clinical information.

A. November 2013 Security Incident:

12. On Monday, November 4, 2013, Horizon BCBSNJ discovered that two (2) unencrypted password-protected laptop computers were stolen from its Newark Office (“November 2013 Incident”).

13. The laptops were issued to two (2) employees with the job title “Writer II” who were employed within Horizon BCBSNJ’s marketing division known as the Enterprise Communication Department.

14. A review of the Writer II job description and Horizon BCBSNJ corporate policy reveals that the employees were not required to store ePHI on their laptops in order to perform their job functions. Horizon BCBSNJ policy in effect at the time of the November 2013 Incident limited employee access to ePHI to the minimum necessary to accomplish an employee's job function.

15. Horizon BCBSNJ's review of the November 2013 Incident revealed that the Horizon BCBSNJ employees did not take their password protected, work-issued laptops home over the weekend. Instead, the laptops were cable-locked to the employees' workstations, which were located on the 8th floor of Horizon BCBSNJ's Newark Office.

16. At the time of the November 2013 Incident, Horizon BCBSNJ was in the process of renovating its Newark Office and moving various employees. Accordingly, over the weekend of November 1, 2013 through November 3, 2013, approximately thirty-two (32) employees of a vendor moving company had restricted access to Horizon BCBSNJ's Newark Office, including the location of the stolen laptops, as part of the renovations and move. In addition, at least 266 other vendors and/or contractors had restricted access to Horizon BCBSNJ's Newark office, including the location of the stolen laptops, during the same time period. A review of surveillance footage from the November 2013 Incident revealed non-Horizon BCBSNJ personnel had unsupervised access to the areas from which the laptops were stolen in order to perform the renovation and moving services.

17. Horizon BCBSNJ's investigation of the November 2013 Incident concluded that one or more of the vendor moving company employees may have stolen the laptops. Horizon BCBSNJ shared its findings with the Newark Police Department; however, no arrests have been made.

18. In the course of its review of the November 2013 Incident, Horizon BCBSNJ's investigation revealed that approximately 109 computers assigned to employees were not equipped with Credant volume encryption software ("Credant Software") as required by Horizon BCBSNJ

corporate policy. Of these 109 computers, thirty-six (36) contained FileVault Mac encryption software, while ten (10) computers were test machines and did not contain ePHI.

19. Following the November 2013 Incident, Horizon BCBSNJ represented that the Credant Software was installed on all company computers within the Enterprise Communications Department.

20. Horizon BCBSNJ's investigation further revealed that the majority of the unencrypted computers were Apple MacBooks procured outside of Horizon BCBSNJ's normal procurement process for the Enterprise Communications Department. Such purchases were not detected by Horizon BCBSNJ's corporate IT department, and as a result, Horizon BCBSNJ's corporate IT department did not adequately monitor, service or install security software required by corporate policy, including the Credant Software.

21. As a result of the Horizon BCBSNJ IT department's lack of monitoring and servicing of MacBooks within the Horizon BCBSNJ Enterprise Communications Department, an unauthorized "shadow IT" department developed with respect to the procurement and servicing of certain Mac devices, which was against Horizon BCBSNJ's existing policies and procedures.

22. Instead of being monitored and serviced by the Horizon BCBSNJ corporate IT department, the MacBooks were monitored by a supervisor of the Enterprise Communications Department. This process was not authorized or approved by Horizon BCBSNJ.

23. As a result of the procurement of the MacBooks outside of Horizon BCBSNJ's established process, certain MacBooks were not configured with approved encryption, data deletion and other software required by corporate policy.

24. Horizon BCBSNJ subsequently retained the computer forensics investigation firm Navigant Consulting, Inc. (“Navigant”) to conduct an investigation to determine the scope of information contained on the stolen laptops and identify the affected members.

25. Navigant’s investigation revealed that the stolen laptops contained the ePHI of approximately 687,838 New Jersey residents, which included member names, addresses, dates of birth, Horizon BCBSNJ identification numbers, and, in some instances, Social Security Numbers and limited clinical information.

26. Horizon BCBSNJ represented that on December 6, 2013, it began notifying affected members by mail and substitute notice in accordance with HIPAA and the New Jersey data breach notification statute, N.J.S.A. 56:8-163. In addition, Horizon BCBSNJ offered affected individuals a free one-year membership in credit monitoring and identity theft protection and restoration services provided by Experian Information Solutions, Inc.

27. On or about December 6, 2013, Horizon BCBSNJ established a dedicated call center to assist impacted members with their questions.

28. On or about December 6, 2013, Horizon BCBSNJ provided notice of the November 2013 Security Incident to the New Jersey State Police, pursuant to N.J.S.A. 56:8-163, the Division, the New Jersey Department of Banking and Insurance, and the United States Department of Health and Human Services, Office for Civil Rights.

29. At the time of the November 2013 Incident, Horizon BCBSNJ’s corporate policy stated that ePHI on portable devices, including laptops and PDAs (including BlackBerry devices), must be encrypted.

B. Additional Security Incidents:

30. Plaintiffs' investigation of the November 2013 Incident revealed that Horizon BCBSNJ had experienced similar laptop thefts and/or other security incidents both prior to and following the November 2013 Incident.

31. On January 7, 2008, Horizon BCBSNJ learned that an IT employee's work-issued, unencrypted laptop was stolen at some point over the prior weekend when the employee had brought the laptop home to complete an assignment ("January 2008 Incident").

32. Horizon BCBSNJ's review of the January 2008 Incident revealed that the Horizon BCBSNJ employee had left the laptop in the trunk of his car in violation of corporate policy while attending a church function in Newark. It is believed that the laptop was stolen at that time.

33. The member data compromised in the January 2008 Incident included the ePHI of approximately 300,000 Horizon BCBSNJ members, including names, Social Security Numbers, addresses and dates of birth. Horizon BCBSNJ represents that the laptop involved in the January 2008 Incident was equipped with Absolute Computrace Software, which, after initiated, would delete all member data if the laptop was connected to the internet.

34. Following the January 2008 Incident, Horizon BCBSNJ corporate policy required all company issued laptops to contain encryption software.

35. On or around May 1, 2008, Horizon BCBSNJ issued a statement for the New Jersey Business Journal's Business Safety and Security Spotlight that it had:

[c]ompleted encryption of all its desktop and laptop computers, as well as its mobile devices in an effort to further protect all data within the company. Horizon BCBSNJ employees have also undergone encryption training so that there is a complete understanding of the new security measures that have been adopted.

36. Following the January 2008 Incident, Horizon BCBSNJ corporate policy required all company issued laptops to contain encryption software.

37. In a separate incident, on or about March 28, 2012, Horizon BCBSNJ discovered that a subcontractor that provided claim processing services to Horizon BCBSNJ included the ePHI of approximately thirteen (13) Horizon BCBSNJ members in a test claim file that was posted to a publicly available website. Access to ePHI was not required for the subcontractor to perform his job duties.

38. In addition, on June 12, 2012, a Horizon BCBSNJ vendor left an unencrypted vendor-issued laptop in a New York taxi cab. The vendor's employee had previously downloaded Horizon BCBSNJ member ePHI onto the lost laptop, against Horizon BCBSNJ policy. Horizon BCBSNJ's review of the incident revealed that the laptop contained the ePHI of approximately eleven (11) New Jersey residents and that the subcontractor did not need access to ePHI to perform his job duties.

COUNT I

VIOLATIONS OF HIPAA

39. Plaintiffs repeat and reallege the allegations in the preceding paragraphs as if more fully set forth herein.

40. At all relevant times, Horizon BCBSNJ is and has been a Covered Entity pursuant to HIPAA, specifically 45 C.F.R. § 160.103.

41. At all relevant times, Horizon BCBSNJ is and has maintained ePHI of New Jersey residents pursuant to HIPAA, specifically 45 C.F.R. § 160.103.

42. As a Covered Entity, Horizon BCBSNJ is required to comply with the HIPAA standards, safeguards and implementation specifications that govern the privacy of ePHI, including the Privacy Rule and the Security Rule. 45 C.F.R. pt. 164, subpts. A, C, & E.

43. As described above, Horizon BCBSNJ failed to comply with the following standards, Administrative Safeguards, Physical Safeguards, Technical Safeguards, and implementation specifications as required by HIPAA, the Privacy Rule and the Security Rule:

- a. Horizon BCBSNJ failed to review and modify security measures as needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).
- b. Horizon BCBSNJ failed to conduct an accurate and thorough risk assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI it held, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).
- c. Horizon BCBSNJ failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).
- d. Horizon BCBSNJ failed to apply appropriate sanctions against workforce members who failed to comply with its security policies and procedures, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(C).
- e. Horizon BCBSNJ failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).
- f. Horizon BCBSNJ failed to implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed, in violation of 45 C.F.R. § 164.308(a)(3)(ii)(A).
- g. Horizon BCBSNJ failed to implement procedures to determine that the access of a workforce member to ePHI is appropriate, in violation of 45 C.F.R. § 164.308(a)(3)(ii)(B).
- h. Horizon BCBSNJ failed to implement policies and procedures that, based upon its access authorization policies, establish, document, review and modify a user's right of access to a workstation, transaction, program or process that includes ePHI, in violation of 45 C.F.R. § 164.308(a)(4)(ii)(C).

- i. Horizon BCBSNJ failed to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that were known to it; and document security incidents and their outcomes, in violation of 45 C.F.R. § 164.308(a)(6)(ii).
- j. Horizon BCBSNJ failed to implement a periodic technical and nontechnical evaluation in response to environmental or operational changes affecting the security of ePHI that establishes the extent to which its security policies and procedures meet the requirements of the Security Rule, in violation of 45 C.F.R. § 164.308(a)(8).
- k. Horizon BCBSNJ failed to implement policies and procedures to safeguard its facility and the equipment therein from unauthorized physical access, tampering and theft, in violation of 45 C.F.R. § 164.310(a)(2)(ii).
- l. Horizon BCBSNJ failed to implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, in violation of 45 C.F.R. § 164.301(a)(2)(iii).
- m. Horizon BCBSNJ failed to implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI, in violation of 45 C.F.R. § 164.310(b).
- n. Horizon BCBSNJ failed to implement physical safeguards for all workstations that access ePHI to restrict access to authorized users, in violation of 45 C.F.R. § 164.310(c).
- o. Horizon BCBSNJ failed to maintain a record of the movements of hardware and electronic media containing ePHI and any person responsible therefore, in violation of 45 C.F.R. § 164.310(d)(2)(iii).
- p. Horizon BCBSNJ failed to implement a mechanism to encrypt and decrypt ePHI, in violation of 45 C.F.R. § 164.312(a)(2)(iv).
- q. Horizon BCBSNJ failed to implement hardware, software and/or procedural mechanisms that record and examine activity that contain or use ePHI, in violation of 45 C.F.R. § 164.312(b).
- r. Horizon BCBSNJ failed to implement policies and procedures to protect ePHI from improper alteration or destruction, in violation of 45 C.F.R. § 164.312(c)(1).

- s. Horizon BCBSNJ failed to implement a mechanism to encrypt ePHI whenever deemed appropriate, in violation of 45 C.F.R. § 164.312(e)(2)(ii).
- t. Horizon BCBSNJ violated the Privacy Rule, 45 C.F.R. § 164.502 et seq.
- u. Horizon BCBSNJ failed to adhere to the minimum necessary standard when using or disclosing protected health information (“PHI”), in violation of 45 C.F.R. § 164.502(b)(1).
- v. Horizon BCBSNJ failed to adequately train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain the security of PHI, in violation of 45 C.F.R. § 164.530(b)(1).
- w. Horizon BCBSNJ failed to reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of the Privacy Rule, in violation of 45 C.F.R. § 164.530(c)(2)(i).
- x. Horizon BCBSNJ failed to apply appropriate sanctions against members of its workforce who failed to comply with its privacy policies and procedures or the requirement of the Privacy Rule, in violation of 45 C.F.R. § 164.530(e)(1).

44. Each violation of the above standards, Administrative Safeguards, Physical Safeguards, Technical Safeguards, and/or implementation specifications by Horizon BCBSNJ constitutes a separate violation of HIPAA on each day the violation continued, 42 U.S.C. § 1320d-5(d)(2); 45 C.F.R. § 160.406.

COUNT II

VIOLATIONS OF THE CFA (UNCONSCIONABLE COMMERCIAL PRACTICES)

45. Plaintiffs repeat and reallege the allegations in the preceding paragraphs as if more fully set forth herein.

46. The CFA, N.J.S.A. 56:8-2, prohibits:

The act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise

47. The CFA defines “merchandise” as “any objects, wares, goods commodities, services or anything offered, directly or indirectly to the public for sale.” N.J.S.A. 56:8-1(c) (emphasis added).

48. At all relevant times, Horizon BCBSNJ has engaged in the advertisement, offer for sale and/or sale of merchandise within the meaning of N.J.S.A. 56:8-1(c), specifically health insurance plans.

49. Horizon BCBSNJ has engaged in unconscionable commercial practices including, but not limited to, each of the above-referenced practices described at Paragraph 43.

50. Each unconscionable commercial practice by Horizon BCBSNJ constitutes a separate violation under the CFA, N.J.S.A. 56:8-2.

COUNT III

VIOLATIONS OF THE CFA **(FALSE PROMISES AND/OR MISREPRESENTATIONS)**

51. Plaintiffs repeat and reallege the allegations in the preceding paragraphs as if more fully set forth herein.

52. Horizon BCBSNJ’s conduct in violation of the CFA includes, but is not limited to, the following false promises and misrepresentations:

- a. Representing that it maintained appropriate Administrative Safeguards, Technical Safeguards and Physical Safeguards to protect its members’ ePHI, when such was not the case.

- b. Representing that all Horizon BCBSNJ laptop computers containing ePHI would be fully encrypted, when such was not the case.
- c. Representing that Horizon BCBSNJ had completed encryption of all laptop computers, when such was not the case.
- d. Representing that all Horizon BCBSNJ employees had been appropriately trained on encryption, when such was not the case.
- e. Following the January 2008 Incident, Horizon BCBSNJ represented it would take additional measures to prevent further laptop thefts. However, such measures were either not taken or ineffective.

53. Each false promise and/or misrepresentation by Horizon BCBSNJ constitutes a separate violation under the CFA, N.J.S.A. 56:8-2.

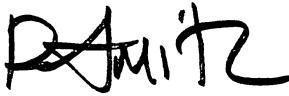
PRAYER FOR RELIEF

WHEREFORE, based upon the foregoing allegations, Plaintiffs respectfully request that the Court enter judgment against Horizon BCBSNJ:

- (a) Finding that the acts and omissions of Horizon BCBSNJ constitute multiple instances of unlawful practices in violation of HIPAA and the CFA;
- (b) Permanently enjoining Horizon BCBSNJ and its owners, officers, directors, employees, representatives, independent contractors, and all other persons or entities directly under its control, from engaging in, continuing to engage in or doing any acts or practices in violation of HIPAA or the CFA, including but not limited to, the acts and practices alleged in this Complaint;
- (c) Directing Horizon BCBSNJ to pay the maximum statutory civil penalties for each and every violation of HIPAA, in accordance with 42 U.S.C. § 1320d-5(d)(2) and 45 C.F.R. § 160.406, and for each and every violation of the CFA, in accordance with N.J.S.A. 56:8-13;
- (d) Directing Horizon BCBSNJ to pay costs and fees, including attorneys' fees as authorized by HIPAA, 42 U.S.C. § 1320d-5(d)(3), and the CFA, N.J.S.A. 56:8-11 and N.J.S.A. 56:8-19; and

- (e) Granting such other relief as the interest of justice may require.

KEVIN JESPERSEN
ACTING ATTORNEY GENERAL OF NEW JERSEY
Attorney for Plaintiffs

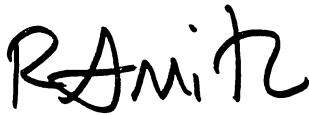
By: 
Elliott M. Siebers
Russell M. Smith, Jr.
Deputy Attorneys General

Dated: February 14, 2017
Newark, New Jersey

RULE 4:5-1 CERTIFICATION

I certify, to the best of my information and belief, that the matter in controversy in this action involving the aforementioned violations of the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 et seq. (“CFA”), and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, as well as the Department of Health and Human Services Regulations, 45 C.F.R. §160 et seq. (collectively, “HIPAA”) is not the subject of any other action pending in any other court of this State. I am aware that an action titled In Re: Horizon Healthcare Services Inc. Data Breach Litigation, United States District Court, District of New Jersey, No. 2:13-cv-07418, has been commenced alleging violations of the CFA and the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (“FCRA”). I further certify, to the best of my information and belief, that the matter in controversy in this action is not the subject of a pending arbitration proceeding in this State, nor is any other action or arbitration proceeding contemplated. I certify that there is no other party who should be joined in this action at this time.

KEVIN JESPERSEN
ACTING ATTORNEY GENERAL OF NEW JERSEY
Attorney for Plaintiffs

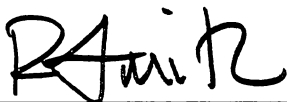
By: 
Russell M. Smith, Jr.
Deputy Attorney General

Dated: February 14, 2017
Newark, New Jersey

RULE 1:38-7(c) CERTIFICATION OF COMPLIANCE

I certify that confidential personal identifiers have been redacted from documents now submitted to the court, and will be redacted from all documents submitted in the future in accordance with Rule 1:38-7(b).

KEVIN JESPERSEN
ACTING ATTORNEY GENERAL OF NEW JERSEY
Attorney for Plaintiffs


By: 
Russell M. Smith, Jr.
Deputy Attorney General

Dated: February 14, 2017
Newark, New Jersey

DESIGNATION OF TRIAL COUNSEL

Pursuant to R. 4:25-4, Deputy Attorney General Russell M. Smith, Jr., is hereby designated as trial counsel for the Plaintiffs in this action.

KEVIN JESPERSEN
ACTING ATTORNEY GENERAL OF NEW JERSEY
Attorney for Plaintiffs

By: 
Russell M. Smith, Jr.
Deputy Attorney General

Dated: February 14, 2017
Newark, New Jersey